International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Detection of Packet Dropping Attacks in Wireless Ad-Hoc Network Based On Privacy Preserving Public Auditing

Kirti B. Mane1[1], N. J. Pathan[2]

[1]PG Student, Department of CSE, M. S. Bidve Engineering College, Latur, Maharashtra, India
[2]Associate Professor, Department of CSE, M. S. Bidve Engineering College Latur, Maharashtra, India

Abstract: ***In multi-hop wireless ad-hoc network packet loss can be caused by mainly because of two different reasons. Link error and malicious packet dropping are two different reasons because of which packet loss can be take place. While discovering continuous packet loss in the network. It is hard to find out whether the loss is due to link error or by malicious packet drop. In this paper we can mainly concentrate on insider attack case that is malicious packet dropping where malicious nodes that are part of the route that will drop a small amount of packet which will affect the network performance. Based on traditional algorithm when we compare the packet dropping rate and the channel error rate, the packet dropping rate does not achieve the satisfactory detection accuracy. To improve the detection accuracy, the correlation between lost packets is identified by using the bitmap obtained from individual node. In this paper a homomorphic linear authenticator which is based on public auditing architecture is applied, which allows the detector to find the truthful information about packet loss. The proposed technique is privacy preserving, collusion proof and causes low communication and storage overheads at intermediate nodes. The auditor will collect the information reported by individual nodes and will determine the reason for packet loss by determining correlation between packet loss. Once the malicious node is identified then it is eliminated from route.***

Keywords: packet dropping, secure routing, attack detection, auditing, correlation, Link error

1. Introduction

WANET is a decentralized type of wireless network. It is used in a network infrastructure and it demands a dynamic network configuration. Since all the nodes in WANET are portable. The nodes are mobile and so that topology is dynamic in nature. The nodes dynamically establish a connection between the source and destination node. Due to multiple hoping structure of wireless ad-hoc network nodes relay on other nodes to forward data packets from source to destination. Malicious nodes can feat this position and disorganize the ad-hoc network operation by dropping data packets and avoiding forwarding them to the next hop. So that completely disrupts the path between the source and destination. At the end such an extreme Denial-of-service (DOS) attack can impair the system by apportioning its topology. In contravention of that diligent packet dropping can practically debase the system execution, from the attackers point of view such a dependably on attack has its weakness. Link error and malicious packet dropping these are the two sources of packet losses. Link errors are the errors obtained due to the harsh channel conditions such as fading, noise and interference. To launch an insider attack, the malicious nodes which are the part of route can explore their knowledge about network protocol and communication context. Such insider attacks can affects the network performance as a persistent attack as much lower risk detecting frequently. A malicious node simply stops forwarding every packet received from upstream node, or may be drop little amount of data which are critical to operation of network or evaluate the importance of packet and interchange some amount of data due to which the risk of network performance. These types of intermittent insider attack may cause considerable damage for the network. To avoid such attacks in this paper we are interested in the problem of routing nodes which are responsible for these drops. In this paper we can develop an appropriate algorithm based on public auditing architecture which can improve the selective packet drop detection accuracy. This algorithm also provides a privacy preserving and truthful decision statistics as a proof to support the detection resolution.

2. Literature Survey

In the year 2000 Xiaobing Zhang, Zhi fu,S. Felix Wu proposed paper titled " Malicious packet dropping: how its impact on TCP performance and how can we detect it." This paper contains three dropping patterns and also can be classified and investigated. To demonstrate attacker which can choose different dropping patterns to degrade the TCP usage to distinct level and selectively drop an excessively small amount of packets. Can results to serve loss to TCP performance. After that, it shows the hacker to utilize a DDOS attack instrument to control an "uncompromising" router to emulate dropping attack. At last, it presents a statistics analysis module for detection of TCP packet dropping attack.

After that in the year 2005 Wenyuam XU, Yanyoung Zhang, Timothy Wood proposed a paper " The possibility of launching and detecting jamming attacks in wireless network" Here we examine the different issues of radio interference attacks. So that to study these issues of directing radio interference attack on remote systems, and also analyze the basic problems of diagnosing the nearness of sticking attacks. Particularly here, proposes four distinct sticking modes of attacks that can be utilized by an enemy to cripple the operations performed in remote system and access their adequacy regarding how every strategy influence the capacity of a remote hub to send and get parcels.

In the year 2009 W.Kozma, and L. Lozos proposed a paper "REAct: Resource efficient accountability for node misbehavior in ad hoc network based on random audits," In order to save the energy or degrade the network performance the misbehaving node may reject to forward or transfer the data packets. This paper investigates the problems of uniquely identifying the set of misbehaving nodes which don't want to forward data to next hop. The new misbehavior identification scheme proposed called REAct i.e. resource efficient accountability for misbehavior node. The identification of misbehaving node can be done with the help of series of random audits triggered upon a performance drop. Based on the behavioral proofs provided by nodes, it is clear that source destination pair using REAct can identify any number of independently misbehaving nodes. These proofs can be constructed using bloom filters which having storage capability and also membership structure. which significantly reducing the communication overhead for misbehavior detection.

In the year 2012 A. proano an L. Lazos," packet hiding method for preventing selective jamming attacks," which investigate problem of the adversary or jammer exploits his internal information for having launching selective jamming attack in which specific massage of high importance are targeted. To prevent these attacks in this paper proposes schemes that prevent real-time packet classification by combing cryptographic primitives with physical layer attributes. Which provides a solution to the selective jamming attack in wireless network would be the encryption of packet that going to sent. First symmetric encryption is applied to the packet data except destination. That means hide the data from adversary. Now MAC header and this permuted data can be again encrypted by using this method. When multi hop communication is applied then intermediate node only required one symmetric decryption to get destination address.

Packet loss = number of packet sent – number of packets received.

By using the above formula the packet loss can be determined. In this way better security against selective jamming attack. Here used the packet hiding method for preventing selective jamming attack.

Summary of Literature Survey

In wireless ad hoc network there are different types of dropping attacks and it is very difficult to handle. In above literature survey we discuss the three packet dropping attacks i.e. random packet dropping, periodic packet dropping and retransmission packet dropping attack. Which are having different patterns causes different levels of damage to TCP performance. Among all these attacks do not cause as much damage as the malicious packet dropping attack. To handle the TCP packet dropping attack problem, here proposed an intrusion detection system approach i.e. TCP dropping statistical analysis module (TDSAM). But this module not yet has been able to prove analytically that, these attack modes capture all types of serious TCP dropping attack. So that here need to plan a countermeasure to defend the QoS against the TCP packet dropping. Due to shared medium of wireless networks the opponents are easily launch jamming attacks. These attacks can interface with the different operations performed in wireless network. For detecting such jamming attacks particularly explore different scenarios but it is not enough to reliably classify the presence of these attacks. After the observation of packet delivery ratio we differentiate between congested and jammed scenarios, here the confusion that the poor link utility is due to presence of jamming or the mobility of node. So that only signal measurement is not sufficient to classify the presence of jammer. To address this need, this paper proposes the two enhanced detection protocols which exercise the consistency checking by constructing prototypes using the MICA2 mote platform which employs the signal strength measurement as well as relative location information. Another problem of packet loss is arising due to the misbehavior node in the wireless ad hoc network. This malicious node may refuse to forward the packets. The previous detection protocols have been tired to address this problem. So that here proposed a novel misbehavior identification scheme called REAct which provides resource efficient accountability for node misbehavior. The different types of packet dropping attacks occur due to the following characteristics of WANET.

Asymmetric links: In wireless ad hoc network nodes are mobile in nature and invariably changing their location within the network.

Routing overheads: In wireless ad-hoc network, nodes frequently change their place within network.

Interference: This is the major problem in wireless network. As links come and go it depends on transmission, if the transmission interrupt with another one can corrupt whole transmission.

Dynamic topology: The topology is not constants, so that mobile node might move and change medium characteristics.
While investigating those attacks and their characteristics, here we can design new security measures to protect (WANET) wireless ad-hoc network
.

3. System Module and Problem Statement

The detection and prevention of selected packet dropping attacks is widely challenging in a highly dynamic environment. These packet dropping attack is specifically due to the open environment of wireless network. We need not only to detect the place of packet drop but also find the cause of packet drop. The packet drop in the WANET could be caused by rough channel conditions ie. link error or by the insider attacker. The detection could be done by independent auditor.Who doesn't know any information held by the node on route. When any misbehaving node is identified auditor should provide a publicly verifiable proof which should be privacy preserving with low communication and storage overheads.

System modules contains four modules

- Setup phase

- Data transmission phase
- Audit phase
- Detection phase

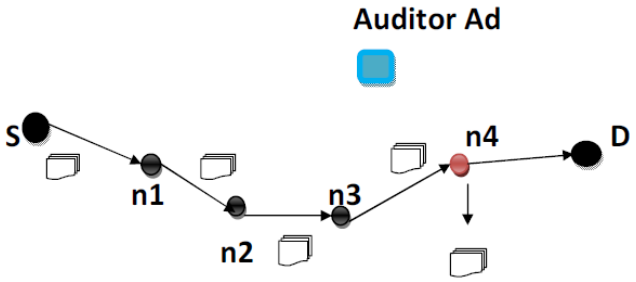

Figure 1: Intermediate nodes with Source and Destination

The above fig.1 shows that the structure of intermediates nodes between source and destination and how the malicious node act and also shows an independent auditor Ad. Node n4 act as an malicious node which can drops the packets received from source. The working of fig.1 can be described below.

- **Setup phase**

In this phase node configuration can be takes place. The source and destination node can be confirmed here. A network is generated by simply connecting nodes with each other. The path PSD is created i.e. (path to source to destination). The S is the upstream node act as source and D is the downstream node act as destination. The packets are sent from source will go through an intermediate node to reach the destination. But before sending the data packets over the path PSD, the source S decides on symmetric key cryptosystem with the help of RSA encryption can be done using public key. S also declares hash function to all nodes in PSD used for authentication purpose.

- **Packet transmission phase**

The completion of the setup phase later on the transmission phase starts. The source S enters in the packet transmission phase before transmitting the packets from source node the packets should be encrypted. This encryption is done with the help of RSA algorithm. The source node should also generate the HLA signature for each packet. The next receiving node will store this packet Pi and HLA signature in the database as a proof of reception and transmission process continues. Here i is nothing but a sequence number that uniquely identifies Pi, S calculates ri = H1(Pi) and generates the HLA signature of ri for node nj, where ri act as receiver, as follows: $Sij = [H2(i||j)uri]x$, for j=1,…k. where || denotes concatenation. These signatures are then sent together with Pi to the route, by using one way chained encryption which prevents the upstream node from deciphering the signature intended to downstream node. Here, each node will create the bitmap. Where **1** indicate that packet has been received successfully and **0** indicate that there has been a packet drop. Using the bitmap created by ACF (autocorrelation function) calculate the correlation between lost packets.

- **Auditing phase**

The auditor Ad is an independent because it does not associated with any node in the network. Also it does not have any information regarding the packet content. The auditor ad is constructed based on HLA (homomorphic linear authenticator). When the source node issues an attack detection request (ADR) the audit phase starts. The ADR message contains the id of the node on PSD, source S HLA public key information, the sequence number of the packets sent by the source S and also sequence number of the packets which are received by the destination D. The auditor ad requests the packet bitmap information from every node in the route. On the basis of information stored on the database, every node on the route will create the bitmap. The auditor checks the validity of the bitmap and accepts if it is valid otherwise, rejects the bitmap and it conclude that not all packets are actually received by the nodes nj. So that node nj is a malicious. We assume that information sent by S and D is truthful because detecting attacks is in their interest.

- **Detection phase**

Phase the auditor ad enters in the detection phase. After receiving and auditing the reply from all nodes on PSD. The main task of the auditor to construct a bitmap for every node and using the ACF (autocorrelation function) the correlation between the lost packets will be calculated. Denoting the lost packet by **'0'** and not lost packets is **'1'**.then checks the difference between calculated value and correlation value of wireless channel. Depending on the comparative difference the auditor takes the decision whether the packets are lost or not over each hop on the route. This is caused by malicious drops. Once malicious node is detected then, it will be excluded from the route and then reset the path.

4. Conclusion

In this paper the result is compared with conventional detecting algorithms. This algorithm uses the classification of the number of lost packets; which can helps to find out the correlation between the lost packets, so that significantly better accuracy in detecting malicious packets drops. Such development is particularly clear if the number of maliciously dropped packets is comparable with those of caused by link errors. For exact calculation of the correlation among those lost packets, it is difficult to achieve truthful packet-loss information at every individual node. To ensure the knowledge about an individual node for packet loss information created is correct or not, here used an HLA based public auditing architecture. This architecture is proven collusion proof, which requires high computational capacity at source node, which incurs low communication and storage overheads in the route.

References

[1] Xiaobing Zhang, TCP Packet Dropping Attacks and Intrusion Detection, M.S. Thesis, North Carolina State University, June, 2000.

[2] M. Allman and V. Paxson, TCP Congestion Control, RFC 2581, April 1999.
[3] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang and W.Weiss, An Architecture for Differentiated Services, RFC 2475, December 1998.
[4] H.–Y. Chang, S.F. Wu and Y.F. Jou, "Real-Time Protocol Analysis for Detecting Link-State Routing Protocol Attacks", ACM Tran. Inf. Sys. Sec., 1, pp. 1-36, 2001.
[5] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in MobiHop Proceedings of the 6th ACM international symposium on Mobile ad hod networking and computing. New York, NY, USA: ACM, 2005.
[6] W. Kozma Jr., and L. Lazos, "REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc. ACM Conf. Wireless Netw. Secur., 2009, pp. 103–110.
[7] Tao Shu and Marwan Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", IEEE Transactions on Mobile Computing, 2012.
[8] Marwan Krunz, Tao Shu, Fellow, IEEE, APRIL 2013 ,"Privacy Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad-Hoc Networks",IEEE Transactions on Mobile Computing , Vol. 14, No. 4
[9] Amutha.S, Balasubramanian.K, "Secure Implementation of Routing Protocols for Wireless Ad hoc Networks" pp. 960-965, Feb 2013.
[10] P. Peethambaran and J. S. Jayasudha, "Survey Of MANET Misbehavior Detection Approaches", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014.

Author Profile

K. B. Mane received the B.E. degree in Computer Science and Engineering from TPCT Engineering College Osmanabad in 2014. Now, she is pursuing Master's in Engineering (Computer Science and Engineering) from M.S. Bidve Engineering college, Latur, SRTM University Nanded, Maharashtra.

N.J. Pathan received the M. Tech. Degrees in Computer Science & Engineering from DR B.A.T.U. Lonere Dist. Raigad. He is now with Computer Science and Engineering of M.S. Bidve Engineering College, Latur as a Associate professor, SRTM University Nanded, Maharashtra.